

# **Reference Manual for the Model CG814M Wireless Cable Modem Gateway**

**NETGEAR**

**NETGEAR, Inc.**  
4500 Great America Parkway  
Santa Clara, CA 95054 USA  
Phone 1-888-NETGEAR

SM-CG814MNA-0  
September 2002

© 2002 by NETGEAR, Inc. All rights reserved.

## **Trademarks**

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

## **Statement of Conditions**

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## **Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## **EN 55 022 Declaration of Conformance**

This is to certify that the CG814M Wireless Cable Modem Gateway is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

## **Bestätigung des Herstellers/Importeurs**

Es wird hiermit bestätigt, daß das CG814M Wireless Cable Modem Gateway gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

## **Certificate of the Manufacturer/Importer**

It is hereby certified that the CG814M Wireless Cable Modem Gateway has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

## **Voluntary Control Council for Interference (VCCI) Statement**

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

## **Customer Support**

Refer to the Support Information Card that shipped with your CG814M Wireless Cable Modem Gateway.

## **World Wide Web**

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) <http://www.netgear.com>. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.



# Contents

<b>About This Manual .....</b>	<b>xi</b>
Audience .....	xi
Typographical Conventions .....	xi
Special Message Formats .....	xii
Technical Support .....	xii
<b>Chapter 1</b>	
<b>Introduction .....</b>	<b>1-1</b>
About the CG814M Gateway .....	1-1
Key Features .....	1-1
Built-in Cable Modem .....	1-1
A Powerful, True Firewall .....	1-2
Content Filtering .....	1-2
802.11b Standards-based Wireless Networking .....	1-2
Configurable Auto Uplink™ Ethernet Connection .....	1-3
USB Port .....	1-3
Protocol Support .....	1-3
Easy Installation and Management .....	1-4
What's in the Box? .....	1-5
The Firewall's Front Panel .....	1-5
The Gateway's Rear Panel .....	1-7
<b>Chapter 2</b>	
<b>Connecting the Gateway to the Internet .....</b>	<b>2-1</b>
What You Will Need Before You Begin .....	2-1
LAN Hardware Requirements .....	2-1
Computer Requirements .....	2-1
LAN Configuration Requirements .....	2-2
Internet Configuration Requirements .....	2-2
Where Do I Get the Internet Configuration Parameters? .....	2-2
Record Your Internet Connection Information .....	2-4

Connecting the CG814M Gateway .....	2-5
Connecting to Your Computer .....	2-5
Ethernet .....	2-6
USB .....	2-6
Wireless .....	2-7
Connecting to your Cable Service Provider .....	2-7
Connecting the Power Adapter .....	2-8
Log in to the Gateway .....	2-8
Connecting the CG814M Gateway to the Internet .....	2-11
Configuration .....	2-11
<b>Chapter 3</b>	
<b>Wireless Configuration.....</b>	<b>3-1</b>
Considerations For A Wireless Network .....	3-1
Security .....	3-1
Placement and Range .....	3-2
Wireless Settings .....	3-2
Wireless Settings .....	3-3
Restricting Wireless Access by MAC Address .....	3-3
Configuring Wired Equivalent Privacy (WEP) .....	3-4
<b>Chapter 4</b>	
<b>Protecting Your Network.....</b>	<b>4-1</b>
Protecting Access to Your CG814M Gateway .....	4-1
Changing the Built-In Password .....	4-1
Blocking Keywords, Sites, and Services .....	4-2
Block Keywords and Domains .....	4-3
Blocking Services .....	4-5
Port Blocking .....	4-6
Port Forwarding .....	4-7
Considerations for Port Forwarding .....	4-9
Port Triggering .....	4-9
Setting Up A Default DMZ Host .....	4-11
Respond to Ping on Internet WAN Port .....	4-11
<b>Chapter 5</b>	
<b>Managing Your Network .....</b>	<b>5-1</b>
Network Status Information .....	5-1

Viewing Gateway Status .....	5-2
Connection Status .....	5-4
Current System Time .....	5-5
Configuring LAN IP Settings .....	5-5
LAN IP Setup .....	5-5
DHCP .....	5-6
Use router as DHCP server .....	5-6
Viewing and Emailing Logged Information .....	5-7
Enabling Logs Event E-mail Notification .....	5-8
Erasing Configuration .....	5-8
Running Diagnostic Utilities .....	5-9
<b>Chapter 6</b>	
<b>Troubleshooting .....</b>	<b>6-1</b>
Basic Functions .....	6-1
Power LED Not On .....	6-2
Test LED Stays On .....	6-2
Local Link LEDs Not On .....	6-2
Cable Link LED Not On .....	6-3
Troubleshooting the Web Configuration Interface .....	6-3
Troubleshooting the ISP Connection .....	6-4
Troubleshooting a TCP/IP Network Using a Ping Utility .....	6-4
Testing the LAN Path to Your Gateway .....	6-4
Testing the Path from Your PC to a Remote Device .....	6-5
<b>Appendix A</b>	
<b>Technical Specifications .....</b>	<b>A-1</b>
<b>Appendix B</b>	
<b>Networks, Routing, and Firewall Basics .....</b>	<b>B-1</b>
Related Publications .....	B-1
Basic Router Concepts .....	B-1
What is a Router? .....	B-2
Routing Information Protocol .....	B-2
IP Addresses and the Internet .....	B-2
Netmask .....	B-4
Subnet Addressing .....	B-5
Private IP Addresses .....	B-7

Single IP Address Operation Using NAT .....	B-8
MAC Addresses and Address Resolution Protocol .....	B-9
Related Documents .....	B-9
Domain Name Server .....	B-10
IP Configuration by DHCP .....	B-10
Internet Security and Firewalls .....	B-10
What is a Firewall? .....	B-11
Stateful Packet Inspection .....	B-11
Denial of Service Attack .....	B-11
Wireless Networking .....	B-12
Wireless Network Configuration .....	B-12
Ad-hoc Mode (Peer-to-Peer Workgroup) .....	B-12
Infrastructure Mode .....	B-12
Extended Service Set Identification (ESSID) .....	B-13
Authentication and WEP Encryption .....	B-13
Wireless Channel Selection .....	B-14
Ethernet Cabling .....	B-15
Uplink Switches and Crossover Cables .....	B-15
Cable Quality .....	B-16
<b>Appendix C</b>	
<b>Preparing Your Network .....</b>	<b>C-1</b>
Preparing Your Computers for TCP/IP Networking .....	C-1
Configuring Windows 95, 98, and ME for TCP/IP Networking .....	C-2
Install or Verify Windows Networking Components .....	C-2
Enabling DHCP to Automatically Configure TCP/IP Settings .....	C-4
Selecting Windows' Internet Access Method .....	C-4
Verifying TCP/IP Properties .....	C-5
Configuring Windows NT, 2000 or XP for IP Networking .....	C-5
Install or Verify Windows Networking Components .....	C-5
Verifying TCP/IP Properties .....	C-6
Configuring the Macintosh for TCP/IP Networking .....	C-6
MacOS 8.6 or 9.x .....	C-6
MacOS X .....	C-7
Verifying TCP/IP Properties for Macintosh Computers .....	C-8
Verifying the Readiness of Your Internet Account .....	C-9

What Is Your Configuration Information? .....	C-9
Obtaining ISP Configuration Information for Windows Computers .....	C-10
Obtaining ISP Configuration Information for Macintosh Computers .....	C-11
Restarting the Network .....	C-12
<b>Glossary</b> .....	<b>G-1</b>



## About This Manual

Thank you for purchasing the NETGEAR™ CG814M Wireless Cable Modem Gateway.

This manual describes the features of the gateway and provides installation and configuration instructions.

## Audience

---

This reference manual assumes that the reader has intermediate to advanced computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices.

## Typographical Conventions

---

This guide uses the following typographical conventions:

<i>italics</i>	Book titles and UNIX file, command, and directory names.
courier font	Screen text, user-typed command-line entries.
Initial Caps	Menu titles and window and button names.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
ALL CAPS	DOS file and directory names.

## Special Message Formats

---

This guide uses the following formats to highlight special messages:



**Note:** This format is used to highlight information of importance or special interest.



**Warning:** This format is used to highlight information about the possibility of injury or equipment damage.



**Danger:** This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.

## Technical Support

---

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at [www.NETGEAR.com](http://www.NETGEAR.com). The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

# **Chapter 1**

## **Introduction**

This chapter describes the features of the NETGEAR CG814M Wireless Cable Modem Gateway.

### **About the CG814M Gateway**

---

The NETGEAR CG814M Wireless Cable Modem Gateway connects directly to the wide area network (WAN) using its built-in cable modem. It has multiple options to connect to your local area network (LAN), including a 4-port 10/100 Mbps Ethernet switch, a USB port and an 802.11b wireless Access Point.

The CG814M Gateway is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the CG814M Gateway uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The CG814M Gateway provides highly reliable Internet access for up to 253 users.

### **Key Features**

---

The CG814M Gateway offers the following features.

#### **Built-in Cable Modem**

The CG814M Gateway connects directly to the WAN using an integrated cable modem. The modem is DOCSIS 1.0 compliant and upgradable to DOCSIS 1.1, guaranteeing that it will work with your local cable service provider.

## A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the CG814M Gateway is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection  
Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Configurable Port Forwarding, Port Blocking, Port Triggering and DMZ provide enough flexibility for most applications.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents  
The CG814M Gateway will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the gateway to email the log to you at specified intervals. You can also configure the gateway to send immediate alert messages to your email address or email pager whenever a significant event occurs.

## Content Filtering

With its content filtering feature, the CG814M Gateway prevents objectionable content from reaching your PCs. The gateway allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the gateway to log and report attempts to access objectionable Internet sites.

## 802.11b Standards-based Wireless Networking

The CG814M Gateway includes an 802.11b-compliant wireless access point, providing continuous, high-speed 11 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11b Standards-based wireless networking at up to 11 Mbps
- 64-bit and 128-bit WEP encryption security
- WEP keys can be generated manually or by passphrase
- Wireless access can be restricted by MAC address.

## **Configurable Auto Uplink™ Ethernet Connection**

With its internal 4-port 10/100 switch, the CG814M Gateway can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the local LAN and the Internet WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

## **USB Port**

A USB connection to your computer eliminates the need for installing an Ethernet card.

## **Protocol Support**

The CG814M Gateway supports the Transmission Control Protocol/Internet Protocol (TCP/IP). [Appendix B, "Networks, Routing, and Firewall Basics"](#) provides further information on TCP/IP.

- IP Address Sharing by NAT

The CG814M Gateway allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached PCs by DHCP

The CG814M Gateway dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- DNS Relay

When DHCP is enabled and no DNS addresses are specified, the gateway provides its own address as a DNS server to the attached PCs. The gateway obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

## **Easy Installation and Management**

You can install, configure, and operate the CG814M Gateway within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management

Browser-based configuration allows you to easily configure your gateway from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.

- Diagnostic functions

The gateway incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the gateway. You can use these diagnostic functions directly from the CG814M Gateway when you are connected on the LAN or when you are connected over the Internet via the remote management function.

- Visual monitoring

The gateway's front panel LEDs provide an easy way to monitor its status and activity.

## What's in the Box?

---

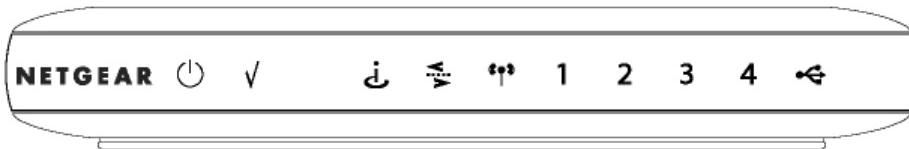
The product package should contain the following items:

- CG814M Wireless Cable Modem Gateway
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- USB cable
- *Resource CD*, including:
  - This manual
  - Application Notes, Tools, and other helpful information
- Warranty and registration card
- Support information card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

## The Firewall's Front Panel

The front panel of the CG814M Gateway ([Figure 1-1](#)) contains status LEDs.



**Figure 1-1: CG814M Gateway Front Panel**

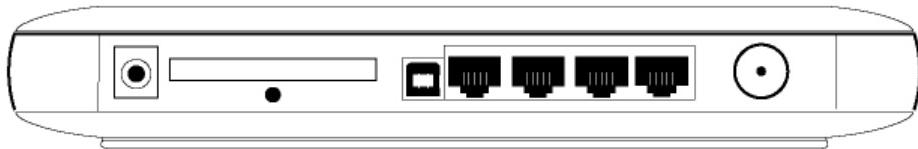
You can use some of the LEDs to verify connections. [Table 1-1](#) lists and describes each LED on the front panel of the CG814M Gateway. These LEDs are green when lit.

**Table 1-1. LED Descriptions**

<b>Label</b>	<b>Activity</b>	<b>Description</b>
Power 	On Off	Power is supplied to the gateway. Power is not supplied to the gateway.
Test 	On Off	A system failure has occurred. Reboot the gateway. Normal operation.
Cable Link 	On (Green) Off	Configuration of the cable interface by your cable service provider is complete. Configuration of the cable interface is still in progress.
Cable Traffic 	On Off	Data is being transmitted or received on the cable interface. The cable interface is idle.
Wireless 	On Blink	Indicates that the wireless Access Point is operating normally. Data is being transmitted or received on the wireless interface.
Local (Local Area Network) 	On (Green) Blink (Green) On (Yellow) Blink (Yellow) Off	The Local port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.
USB 	On (Green) Blink (Green) Off	The Local port has detected link with a USB device. Data is being transmitted or received through USB. No link is detected on the USB port.

## The Gateway's Rear Panel

The rear panel of the CG814M Gateway ([Figure 1-2](#)) contains the connections identified below.



**Figure 1-2: CG814M Gateway Rear Panel**

Viewed from left to right, the rear panel contains the following elements:

- AC power adapter input
- 802.11b Wireless antenna
- Factory Default Reset push button
- USB port for connecting the gateway to the local computer
- Four Local Ethernet RJ-45 ports for connecting the gateway to the local computers
- Coaxial F-type connector for connecting the gateway directly to your cable service provider



## **Chapter 2**

# **Connecting the Gateway to the Internet**

This chapter describes how to set up the CG814M Gateway on your Local Area Network (LAN), connect to the Internet and perform basic configuration.

### **What You Will Need Before You Begin**

---

You need to prepare these three things before you can connect your gateway to the Internet:

1. A computer properly connected to the gateway as explained below.
2. Active Data Over Cable Internet service provided by cable modem account.
3. The Internet Service Provider (ISP) configuration information for your cable modem account.

### **LAN Hardware Requirements**

The CG814M Gateway connects to your LAN using either its twisted-pair Ethernet, USB or 802.11b wireless port.

### **Computer Requirements**

To use the CG814M Gateway on your network, each computer must have either an installed Ethernet Network Interface Card (NIC) , USB Host port or 802.11b wireless adapter. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your gateway.

## **LAN Configuration Requirements**

For the initial connection to the Internet and configuration of your gateway, you will need to connect a computer to the gateway which is set to automatically get its TCP/IP configuration from the gateway via DHCP.

**Note:** Please refer to [Appendix C, "Preparing Your Network"](#) for assistance with DHCP configuration.

## **Internet Configuration Requirements**

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your gateway to the Internet:

- Host and Domain Names
- ISP Domain Name Server (DNS) Addresses
- Fixed or Static IP Address

If you already have cable Internet service and are replacing a cable modem, you may need these parameters.

- CG814M Gateway Cable and Device MAC Address, that can be found on the bottom of your gateway, or on the Basic Settings page.
- The MAC Address of the PC that you use to access the internet.

### **Where Do I Get the Internet Configuration Parameters?**

There are several ways you can gather the required Internet connection information.

- Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Macintosh computers, open the TCP/IP or Network control panel.

- You may also refer to the *CG814W Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

## Record Your Internet Connection Information

1. Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

**Fixed or Static IP Address:** If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Subnet Mask: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Gateway IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

**ISP DNS Server Addresses:** If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Secondary DNS Server IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

**Host and Domain Names:** Some ISPs use a specific host or domain name like **CCA7324-A** or **attbi**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: \_\_\_\_\_ ISP Domain Name: \_\_\_\_\_

**MAC Addresses of CG814M Gateway and PC:** If you have existing cable internet service and are replacing your cable modem you may need to notify your cable service provider of the MAC Address (often called Hardware Address) and/or Device Address of your CG814M Gateway. The Device Address is the equivalent of a PC behind the cable modem, and can be "cloned". Cloning allows you to specify the MAC address of the packets the gateway sends to the internet. If you clone the MAC Address of your PC you will not have to register the Device Address of your gateway.

Cable Modem MAC (listed on the bottom of your gateway): \_\_\_\_\_

Device MAC (listed on the bottom of your gateway): \_\_\_\_\_

PC MAC Address (listed on the Basic Settings page): \_\_\_\_\_

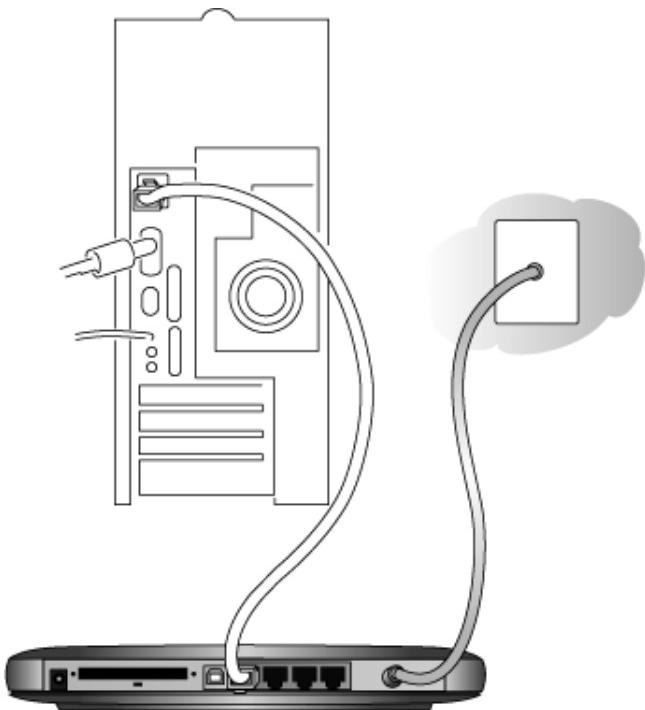
## Connecting the CG814M Gateway

---

Before using your modem, you need to do the following:

- Connect to your computer, using either Ethernet, USB or wireless (see [page 2-6](#)).
- Connect the line from your cable service provider to the cable port of the gateway (see [page 2-7](#)).
- Connect the power adapter (see [page 2-8](#)).

A typical installation is shown in [Figure 2-1](#), below



**Figure 2-1: Typical installation using Ethernet.**

## Connecting to Your Computer

Your computer will attach to either the Ethernet, USB or wireless ports on the CG814M Gateway.

## Ethernet

To connect your computer to the modem via Ethernet:

1. Locate the Category 5 Ethernet cable which came with your modem.
2. Connect your computer to the modem using the Ethernet cable.:



**Note:** The CG814M Gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a switch or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

## USB

To connect your computer to the modem via USB involves installing the USB driver:



**Note:** The USB connection option is only available for Windows PCs. Also, Windows 95 does not support USB without special operating system upgrades and patches.

1. Install the USB driver
  - a. Insert the CD which came with your modem into the CD drive of your computer.
  - a. Connect the USB cable to your modem and plug in the AC power for the modem.
  - b. Use the USB cable to connect your computer to the modem.

The found new hardware Windows installation wizard will prompt you for the drivers.



Browse to the CD and install the USB driver by clicking through the Windows wizard prompts.

## Wireless

Detailed instructions on configuring your wireless devices for TCP/IP networking are provided in the next chapter. However, if you already have a functioning wireless network and you wish to use a wireless PC to initially configure the router, you will need to change the settings of that PC to match the default settings of the router:

- The SSID should be **Wireless** (note the capitalization).
- The Channel should be set to **6**.
- WEP encryption is disabled.

## Connecting to your Cable Service Provider

Using a coaxial cable provided by your cable service provider, connect the coaxial cable jack on your wall to the cable connector on the gateway.

The Cable Link LED will be solid green when your gateway has synchronized with the cable headend.

## Connecting the Power Adapter

To connect the power adapter to the gateway:

1. Plug the connector of the power adapter into outlet on the rear panel of the modem.
2. Plug the other end of the adapter into an AC power outlet.
3. Verify that the PWR LED on the modem is lit.

After applying power to the gateway, complete the following steps to verify that power is correctly applied:

1. When power is first applied, verify that the Power LED comes on.  
All the numbered LAN LEDs will be briefly tested.
2. After approximately 10 seconds, verify that the local Ethernet or USB port LED is lit for the port that is connected to your computer.

If a port's LED is lit, a link has been established to the connected device. If a local Ethernet port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED should be yellow.

## Log in to the Gateway

---



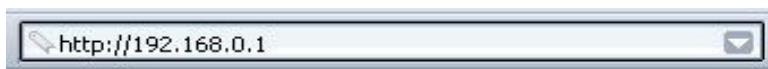
**Note:** To connect to the gateway, your computer needs to be configured to obtain an IP address automatically via DHCP. Please refer to [Appendix C, "Preparing Your Network"](#) for instructions on how to do this.

1. Turn on the gateway.
2. Now, turn on your computer.

**Note:** If you usually run software to log in to your Internet connection, do not run that software.

Now that the gateway, and the computer are turned on, verify the following:

- When power on the gateway was first turned on, the PWR light went on, the numbered LAN LEDs turned on for a few seconds.
  - The gateway's LOCAL LINK/ACT lights are lit for any computers that are connected to it.
  - The gateway's Cable Link LED is lit, indicating a link has been established to the cable service provider.
3. Next, use a browser like Internet Explorer or Netscape to log in to the gateway at its default address of <http://192.168.0.1>.



**Figure 2-2: Log in to the gateway**

A login window opens as shown in [Figure 2-3](#) below:



**Figure 2-3: Login window**

For security reasons, the gateway has its own user name and password. When prompted, enter **admin** for the gateway User Name and **password** for the gateway Password, both in lower case letters..



**Note:** The user name and password are not the same as any user name or password you may use to log in to your Internet connection.

#### 4. Connect to the Internet

The screenshot shows the 'Connection' page of the NETGEAR CG814W. On the left, a sidebar lists various configuration categories: Setup, Content Filtering, Logs, Block Sites, Services, Maintenance, Gateway Status, Connection, Set Password, Diagnostics, Advanced, MAC Filtering, Port Forwarding, DMZ Host, and LAN IP. The main content area is titled 'Connection'. It includes three tables: 'Startup Procedure', 'Downstream Channel', and 'Upstream Channel'. The 'Startup Procedure' table has four rows: Acquire Downstream Channel (Status: Locked), Connectivity State (OK, Operational), Boot State (OK, Operational), and Configuration File (Security: Disabled). The 'Downstream Channel' table has five rows: Lock Status (Locked), Channel ID (1), Modulation (QAM64), Symbol rate (5056941), and Downstream Frequency (21.2 dBmV). The 'Upstream Channel' table has five rows: Lock Status (Locked), Channel ID (1), Modulation (QPSK), Symbol rate (1280 Ksym/sec), and Upstream Frequency (0.0 dBmV). To the right of the tables is a 'Connection Help' section with a note about tracking initialization procedures and a bullet point about current system time.

Figure 2-4: Connection page.

You are now connected to the gateway's *Connection* page, shown in [Figure 2-4](#). This page provides detailed information about your cable connection.



**Note:** If you were unable to connect to the gateway, please refer to “[Basic Functions](#)” on [page 6-1](#).

## Connecting the CG814M Gateway to the Internet

The gateway is now properly attached to your network. You are ready to configure your gateway to connect to the Internet. To continue installation, click on the *Basic Settings* menu, shown in Figure 2-5..

### Basic Settings

---

**Network Configuration**

WAN IP Address:	<b>10.152.152.214</b>
Duration	<b>D: 06 H: 23 M: 59 S: 58</b>
Expires	<b>MON SEP 30 10:59:58 2002</b>
Host Name	<input type="text" value="atb1.com"/> (Required by some ISPs)
Domain Name	<input type="text" value="atb1.com"/> (Required by some ISPs)
<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP	
Dynamic IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
MAC Address	<b>00:09:5b:19:02:2e</b>
Cloned MAC Address	<input type="text" value="00"/> : <input type="text" value="10"/> : <input type="text" value="95"/> : <input type="text" value="0d"/> : <input type="text" value="02"/> : <input type="text" value="6e"/>

---

**Firewall Protection**  *Enable*

---

**Figure 2-5: Browser-based configuration Basic Settings menu**

Unless your ISP assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP you recorded in “[Record Your Internet Connection Information](#)” on page 2-4.

## Configuration

1. Your current WAN IP address is shown on this page.

If you have set your configuration for Dynamic IP, below, then an IP address shown here is an indication that you have successfully received an IP address from your service provider.

If you have set your configuration to Static IP, below, then the IP address you entered will be shown here.

For Dynamic IP, the Duration and time of Expiration of the IP address are shown. The IP address is renewed automatically using DHCP.

2. Enter your Host Name and Domain Name.

These parameters may be necessary to access your ISP's services such as mail or news servers.

3. Select Dynamic or Static IP Address:

If your service provider assigns your IP address automatically through DHCP, select "Dynamic IP". If your service provider has assigned you a permanent, fixed (static) IP address for your PC, select "Static IP".

If you select Static IP, enter the IP address that your ISP assigned. Also enter the Static IP Mask (also known as netmask), Gateway IP address and Domain Name Server (DNS) Addresss.

The Gateway is the ISP's router to which your gateway will connect.

A DNS server is a host on the Internet that translates Internet names (such as [www.netgear.com](http://www.netgear.com)) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your gateway during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the gateway.

4. Cable MAC Address:

Device MAC Address

This section indicates the Cable and Device MAC Address settings of your gateway. If you have existing cable internet service and are replacing your cable modem you may need to notify your cable service provider of the Cable MAC Address and/or Device MAC Address of your gateway in order to obtain service. The CG814M Gateway appears to your service provider to be a cable modem with a single PC connected to it. The Cable Address is the equivalent of the cable modem. The Device Address is the equivalent of the PC behind the cable modem, and can be "cloned". Cloning allows you to specify the MAC address of the packets the gateway sends to the internet. If you clone the MAC Address of your PC you will not have to register the Device Address of your gateway.

To change the Device MAC Address that is used to send traffic to the internet, enter the MAC address you would like to use in the "Cloned MAC Address" field and check the Enable box. The MAC Address that is entered by default is the MAC Address of the PC that is accessing the gateway's web interface.

5. Firewall Protection:

Normally firewall protection should be enabled to protect your network from attacks from the internet. Removing the check from the “Firewall Protection” box disables your firewall.

6. Click Apply to save your settings.



## Chapter 3

# Wireless Configuration

This chapter describes how to configure the wireless features of your CG814M Wireless Cable Modem Gateway.



**Note:** If you are configuring the gateway from a wireless PC and you change the gateway's SSID, channel, or WEP settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your PC to match the gateway's new settings.

## Considerations For A Wireless Network

---

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your gateway in order to maximize the network speed. For further information on wireless networking, refer to “[Wireless Networking](#)” in [Appendix B, "Networks, Routing, and Firewall Basics"](#).

## Security

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, NETGEAR strongly recommends that you make use of the security features of your wireless equipment. As a minimum security precaution, you should change the SSID setting of all devices on your network from the factory setting to a unique password. Restricting access by MAC address filtering adds another obstacle against unwanted hosts joining your network. To hinder a determined eavesdropper, you should enable Wired Equivalent Privacy (WEP) data encryption.

## Placement and Range

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless gateway. For best results, place your gateway:

- near the center of the area in which your PCs will operate,
- in an elevated location such as a high shelf,
- away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- away from large metal surfaces.

## Wireless Settings

---

To configure the Wireless interface of your gateway, click on the Wireless Settings heading in the Setup section of the browser interface. The Wireless Settings menu will appear, as shown in [Figure 3-1](#):

**Wireless Settings**

---

**Identification**

Regulatory Domain: USA/Canada  
Station Name: FR114W  
SSID (Service Set Identifier):

---

**Options**

Channel No:

WEP Status: no data encryption

---

**Access Point**

Allow access by:  Everyone  Trusted PCs only

---

**Figure 3-1: Wireless Settings menu**

## Wireless Settings

In the Wireless Settings section are the following parameters:

- Name (SSID)

Enter a Service Set ID (SSID) value of up to 32 alphanumeric characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is **Wireless**, but NETGEAR strongly recommends that you change your network's SSID to a different value.

- Channel

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

## Restricting Wireless Access by MAC Address

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses.

Check the Turn Access Control On box to restrict access to your network to computers in the Access Control List.

To access the Access List, click the Setup Access List button shown in [Figure 3-2](#):

**Wireless Card Access List**

---

#	Device Name	Mac Address
<input checked="" type="radio"/> 1	Sanders	12:34:56:78:90:12
<input type="radio"/> 2	James	98:76:54:32:10:98

**Add** | **Edit** | **Delete**

---

**Apply** | **Cancel**

**Figure 3-2: Wireless Access List menu**

The Wireless Access window displays a list of MAC addresses that will be allowed to connect to the gateway. These PCs must also have the correct SSID and WEP settings. To restrict access based on MAC addresses:

1. Click the Add button to go to the Add/Edit menu.

For your convenience, this menu displays a list of currently active wireless cards and their MAC addresses.

2. If the desired PC appears in the list, you can click on it to capture its MAC address; otherwise, you can manually enter the MAC address of the authorized PC.  
The MAC address is usually printed on the wireless card.

3. If no Device Name appears, you can type a descriptive name for the PC that you are adding.
4. Click Add.
5. When you have finished entering MAC addresses, return to the Wireless Access List menu and check the Turn Access Control On box, then click Apply.

To edit a MAC address from the table, click on it to select it, then click the Edit or Delete button.



**Note:** If the **Turn Access Control On** is enabled and the Access Control List is blank; then all wireless PCs will be unable to connect to your wireless network.

## Configuring Wired Equivalent Privacy (WEP)

In the Wireless Settings menu you can configure WEP data encryption from the Security Encryption (WEP) section using the following parameters:

- Encryption Mode  
Select the WEP Encryption level:
  - Off - no data encryption (Open System)
  - 64-bit (sometimes called 40-bit) encryption
  - 128-bit encryption
- Authentication Type  
Select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.
- Keys  
If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
- Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)  
Select which of the four keys will be active.

Be sure to click Apply to save your settings in this menu.



# Chapter 4

## Protecting Your Network

This chapter describes how to use the firewall features of the CG814M Wireless Cable Modem Gateway to protect your network.

### Protecting Access to Your CG814M Gateway

---

For security reasons, the gateway has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the gateway User Name and **password** for the gateway Password. You can use procedures below to change the gateway's password and the amount of time for the administrator's login timeout.

**Note:** The user name and password are not the same as any user name or password you may use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

### Changing the Built-In Password

1. Log in to the gateway at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.



Figure 4-1: Log in to the gateway

- From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in **Figure 4-2**.

The screenshot shows a 'Maintenance' menu on the left with options: Gateway Status, Connection, Set Password, and Diagnostics. The 'Set Password' option is highlighted. To its right is the 'Set Password' configuration page. It has two input fields: 'Password' and 'Re-Enter Password', both showing masked text. Below these is a 'Restore Factory Defaults' section with radio buttons for 'Yes' and 'No', where 'No' is selected. At the bottom is a large 'Apply' button.

**Figure 4-2: Set Password menu**

- To change the password, first enter the old password, and then enter the new password twice.
- If you would like to reset your gateway to its factory default settings select Yes for Restore Factory Defaults. This will remove all configuration information you have entered.
- Click Apply to save your changes.

**Note:** After changing the password, you will be required to log in again to continue the configuration. If you have backed up the gateway settings previously, you should do a new backup so that the saved settings file includes the new password.

## **Blocking Keywords, Sites, and Services**

---

The gateway provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the CG814M Gateway prevents objectionable content from reaching your PCs. The CG814M allows you to control access to Internet content by screening for keywords within Web addresses. It also has the capability to block access to all sites except those that are explicitly allowed. Key content filtering options include:

- Blocking access from your LAN to Internet locations that contain keywords that you specify.
- Blocking access to web sites that you specify as off-limits.

- Allowing access to only web sites that you specify as allowed.
- Filtering of Proxy servers, Cookies, Java, ActiveX and Popup Windows

The section below explains how to configure your gateway to perform these functions.

## **Block Keywords and Domains**

The CG814M Gateway allows you to restrict access to Internet content based on functions such as web address keywords and web domains.

A domain name is the name of a particular web site. For example, for the address www.NETGEAR.com, the domain name is NETGEAR.com.

Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

1. Click on the Block Sites link of the Content Filtering menu.

The screenshot shows the 'Block Sites' configuration page. On the left, a sidebar lists 'Content Filtering' with options for 'Logs', 'Block Sites', and 'Services'. The main area is titled 'Block Sites' and contains three sections: 'Keyword Blocking', 'Domain Blocking', and a time-based blocking section.

**Keyword Blocking:** An enable checkbox is checked. A text input field contains the word 'violence'. Below it are 'Add Keyword' and 'Remove Keyword' buttons.

**Domain Blocking:** An enable checkbox is checked. A radio button is selected for 'Deny Domains' over 'Allow Domains'. A text input field contains 'playboy.com'. Below it are 'Add Domain' and 'Remove Domain' buttons.

**Time-Based Blocking:** Options include 'Always block' (radio button), 'block from 10:00 to 16:30' (radio button selected, with dropdowns for hours and minutes), and a day range selector showing 'Monday through Friday'.

**Figure 4-3: Block Sites menu**

2. To enable keyword blocking or Domain Blocking, check the appropriate Enable box.

3. Enter Keywords into the Keyword List by typing then in the Add Keyword box, then, click Add Keyword.

Some examples of Keyword applications follow:

- If the keyword “XXX” is specified, the URL <<http://www.badstuff.com/xxx.html>> is blocked.
- If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- Enter the keyword “.” to block all Internet browsing access.

Up to 8 entries are supported in the Keyword list.

4. Enter Domains into the Domain List by typing then in the Add Domain box, then, click Add Domain.

If the domain “badstuff.com” is specified, the URL <<http://www.badstuff.com/xxx.html>> is blocked, along with all other urls in the badstuff.com site.

Up to 8 entries are supported in the Keyword list.

5. To block access to the domains in the Domain List, select Deny Domains.

To allow access to only the domains in the Domain List, select Allow Domains. If the domain “goodstuff.com” is specified, you will be able to access only sites on the goodstuff site.

6. To delete a keyword or domain, select it from the list, click Remove Keyword or Remove Domain.

7. Configure the times when access rules apply in the Schedule section.

8. Click Apply to save your settings.

## **Blocking Services**

The CG814M Gateway allows you to block access to specific traffic such as proxies, cookies, Java Applets, ActiveX and popup windows.

To enable filtering of services, from the Content Filtering section of the Main Menu, select Services. Check the Enable box for whichever service you would like to block and click Apply.

### **Proxy**

The proxy filter will prevent PCs from using a proxy server to surf the web. A proxy server could be used to bypass parental control features because the port number for a proxy is usually 8080.

Most web surfing is done on port 80. The parental control feature monitors port 80 so proxy based web surfing would not be inspected by the parental controls. The proxy filter should be used if parental controls are being used.

## **Cookies**

A cookie is a text file saved by your web browser which is sent to a particular web server every time you visit the site. Cookies are used to identify you to the web server automatically.

## **Java Applets**

Java Applets are programs that run from within another application, such as a web browser.

## **ActiveX**

An ActiveX control is a Microsoft Windows program that can be downloaded from a web page and automatically executed by your web browser on your PC.

## **Popup Windows**

Many internet sites open additional browser windows, called popups. They are often used for advertisements. The CG814M can filter out many of these popup windows.

# **Port Blocking**

---

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Instructions for setting up inbound rules can be found in “[Port Forwarding](#)” on page -7. Outbound rules (LAN to WAN) determine what outside resources local users can have access to. This section describes how to set up outbound rules.

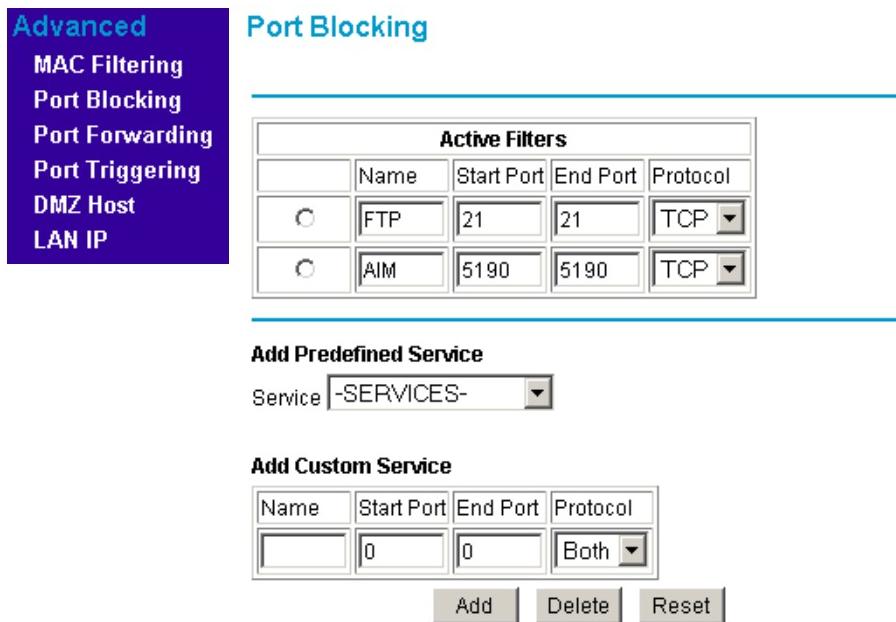
A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the CG814M Gateway are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

You may define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the

rule you have defined.

To configure outbound rules on the CG814M Gateway, click the Port Blocking link on the Advanced section of the main menu.



**Figure 4-4: Port Blocking menu**

- To block outbound traffic, select the service you would like to block from the drop-down list of predefined services. Click Add.
- If the service you would like to block is not in the predefined list, you can add a custom service. Enter the range of ports you would like to block and select whether the ports are TCP, UDP or Both. Click Add.
- To delete an existing rule, select its button on the left side of the table and click Delete.

## Port Forwarding

---

Because the CG814M Gateway uses Network Address Translation (NAT), your network presents

only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule tells the gateway to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as Port Forwarding.



**Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

To configure inbound rules on the CG814M Gateway, click the Port Forwarding link on the Advanced section of the main menu..

Active Forwarding Rules					
	Name	Start Port	End Port	Protocol	Local IP Address
<input type="radio"/>	TELNET	23	23	TCP	192.168.0.10
<input type="radio"/>	HTTP	80	80	TCP	192.168.0.15

Choose Predefined Service  
Service: -SERVICES-

Add Custom Rules

Name	Start Port	End Port	Protocol	Local IP Address
	0	0	Both	192.168.0.0

Add    Delete    Reset

**Figure 4-5: Port Forwarding menu**

- To forward inbound traffic:

1. Select the service you would like to forward from the drop-down list of predefined services.  
If the service you would like to forward is not in the predefined list, you can add a custom service. Enter the range of ports you would like to forward and select whether the ports are TCP, UDP or Both.
  2. Enter the IP address of the computer on your network to which you would like to direct the inbound traffic
  3. Click Add.
  4. To access the local computer from the Internet, you must use the WAN address of your gateway, which can be found on the Basic Settings page.
- To delete an existing rule, select its button on the left side of the table and click Delete.

## **Considerations for Port Forwarding**

If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menus so that external users can always find your network.

- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, you can assign a static IP address to your server outside the range that is assigned by DHCP, but in the same subnet as the rest of your LAN. By default, the IP addresses in the range of 192.168.0.2 through 192.168.0.9 are reserved for this.
- Local PCs must access the local server using the PCs' local LAN address (192.168.0.XXX, by default). Attempts by local PCs to access the server using the external WAN IP address will fail.

## **Port Triggering**

---

Port Triggering is an advanced feature that allows you to dynamically open inbound ports based on outbound traffic on different ports. This is an advanced feature that can be used for gaming and other internet applications.

Port Forwarding can typically be used to enable similar functionality, but it is static and has some limitations. Ports will be open to traffic from the internet until the port forwarding rule is removed. Additionally, port forwarding does not work well for some applications when your WAN IP address is assigned by DHCP, and is changed frequently. Port Triggering opens incoming port temporarily and can does not require the server on the internet to track your IP address if it is

changed.

Port Triggering monitors outbound traffic. When the gateway detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and “triggers” the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

An example of Port Triggering for Internet Relay Chat (IRC) is shown in [Figure 4-6](#). When you connect to an IRC server, the server tries to connect back on port 113 to do an Ident lookup. Unless you have configured Port Forwarding to open port 113, the traffic will be blocked. In this example, the initial login to the server in the range of ports 6660 to 6670 will be detected. This will trigger the gateway to temporarily forward port 113 to the PC that initiated the login.<sup>1</sup>

The screenshot shows the 'Port Triggering' configuration page. On the left, a sidebar lists 'Advanced' options: MAC Filtering, Port Blocking, Port Forwarding, Port Triggering (which is selected and highlighted in blue), DMZ Host, and LAN IP. The main area is titled 'Port Triggering' and contains a table with 10 rows for configuring port triggers. The table has columns for 'Trigger Range' (Start Port, End Port) and 'Target Range' (Start Port, End Port), both of which are currently set to 113. The 'Protocol' column is set to TCP, and the 'Enable' column has a checked checkbox for the first row. Below the table are three buttons: 'Apply', 'Delete', and 'Reset'.

	Trigger Range		Target Range		Protocol	Enable
	Start Port	End Port	Start Port	End Port		
<input type="radio"/>	6660	6670	113	113	TCP	<input checked="" type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>

**Figure 4-6: Port Triggering menu, with IRC example.**

To configure Port Triggering:

1. In the Trigger Range, enter the outbound ports that will be monitored for activity. This will be the “trigger”.
2. In the Target Range, enter the inbound ports that should be forwarded when the trigger occurs.
3. Select the appropriate protocol: TCP, UDP or Both.
4. Check the Enable box
5. Click Apply

To clear a Port Triggering rule, you can either remove the check from the Enable box, to temporarily disable the rule, or you can select the rule and click Delete.

## **Setting Up A Default DMZ Host**

---

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The gateway is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC’s IP address is entered as the Default DMZ Host.



**Note:** For security, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the gateway unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding or Port Triggering menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Host.

To assign a computer or server to be a DMZ Host, from the Main Menu, under Advanced, select DMZ Host. Enter the IP address of the computer you would like to assign as a DMZ Host and click Apply. To disable the DMZ Host, enter “0” and click Apply.

## **Respond to Ping on Internet WAN Port**

---

If you want the gateway to respond to a ‘ping’ from the Internet, click the ‘Respond to Ping on

WAN Port' check box. This should only be used as a diagnostic tool, since it allows your gateway to be discovered. Don't check this box unless you have a specific reason to do so.

## **Chapter 5**

# **Managing Your Network**

This chapter describes how to perform network management tasks with your CG814M Wireless Cable Modem Gateway.

### **Network Status Information**

---

The CG814M provides a variety of status and usage information which is discussed below.

## Viewing Gateway Status

From the Main Menu, under Maintenance, select Gateway Status to view the screen in [Figure 5-1](#).

The screenshot shows the 'Gateway Status' screen with a sidebar menu titled 'Maintenance' containing 'Gateway Status', 'Connection', 'Set Password', and 'Diagnostics'. The main area has two tables:

Information	
Standard Specification Compliant	DOCSIS 1.0/1.1
Hardware Version	3
Software Version	2.64i.2
Cable Modem MAC Address	00:09:5b:19:02:2a
Cable Modem Serial Number	
CM certificate	Installed

Status	
System Up Time	0 days 00h:02m:39s
Network Access	Allowed
Cable Modem IP Address	10.151.141.11

**Figure 5-1: Gateway Status screen**

This screen shows the following parameters:

**Table 5-1.     Menu 3.2 - Router Status Fields**

Field	Description
Information	
Standard Specification Compliant	The specification to which the gateway's cable interface is compatible.
Hardware Version	The hardware version of the gateway.
Software Version	The software version of the gateway.
Cable Modem MAC Address	The MAC address being used by the Cable Modem port of the gateway. This MAC address may need to be registered with your Cable Service Provider.
Cable Modem Serial Number	The serial number of the gateway hardware.

**Table 5-1.     Menu 3.2 - Router Status Fields**

Field	Description
CM Certificate	If the Cable Modem certificate is Installed, it is possible for the service provider to upgrade your Data Over Cable service securely.
Status	
System Up Time	This is the time since the gateway has registered with your cable service provider.
Network Access	This field will change to Allowed when the registration with your cable service provider is complete.
Cable Modem IP Address	The IP address of your gateway, as seen from the Internet.

## Connection Status

From the Main Menu, under Maintenance, select Connection to view the screen in Figure 5-2.

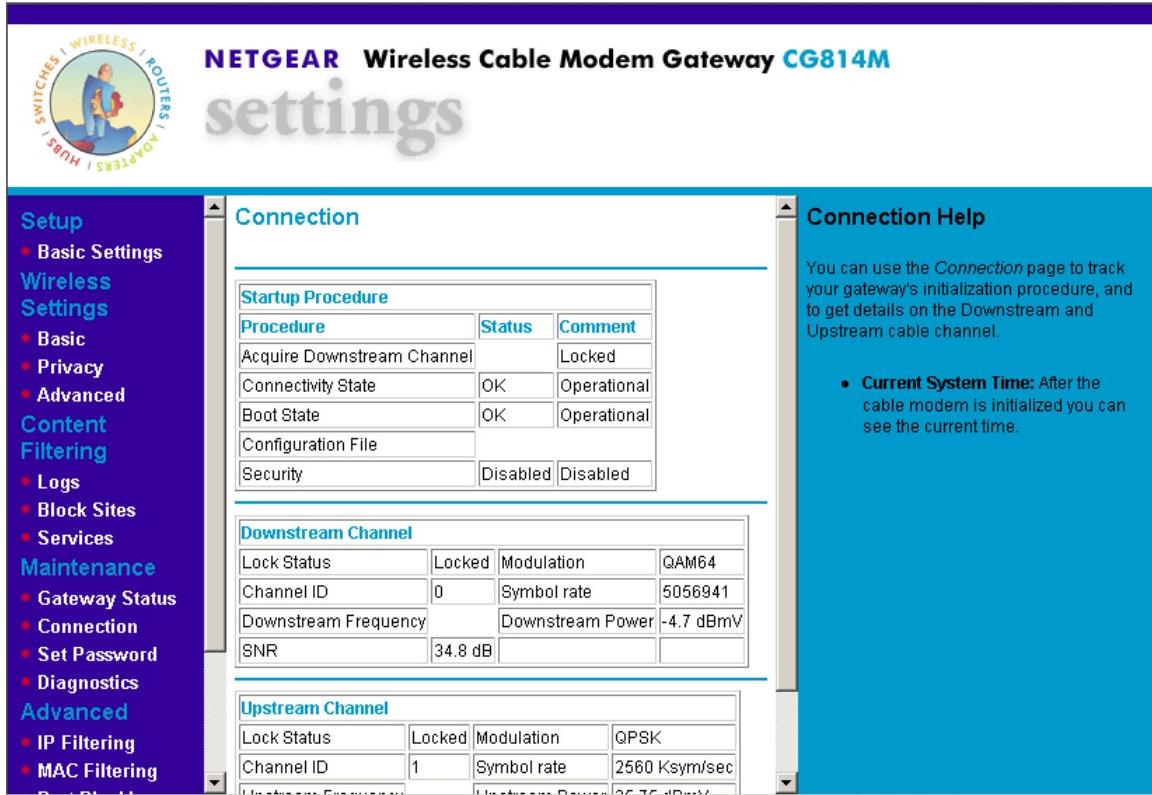


Figure 5-2: Connection screen

This screen shows detailed information about the status of the connection to your cable service provider that can be used for troubleshooting. The gateway goes through the following steps to be provisioned

1. Acquire and lock Downstream Channel
2. Acquire upstream parameters and range.
3. Lock Upstream Channel
4. Acquire IP Address through DHCP

## **Current System Time**

The date and time is acquired from your cable service provider as part of the registration procedure.

## **Configuring LAN IP Settings**

---

The LAN IP Setup menu allows configuration of LAN IP services such as the IP address of the gateway and DHCP. These features can be found under the Advanced heading in the Main Menu in the LAN IP menu.

### **LAN IP Setup**

The gateway is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The gateway's default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN TCP/IP Setup parameters are:

- LAN IP Address  
This is the IP address of the gateway.
- Subnet Mask  
This is the LAN Subnet Mask of the gateway. Combined with the IP address, the Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.



**Note:** If you change the LAN IP address of the gateway while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

## DHCP

By default, the gateway will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the gateway. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the gateway are satisfactory. See “[IP Configuration by DHCP” on page B-10](#)” for an explanation of DHCP and information about how to assign IP addresses for your network.

### Use router as DHCP server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, select NO for the DHCP Server, otherwise leave Yes selected.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the gateway's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.10 and 192.168.0.253. The range of IP addresses between 192.168.0.2 and 192.168.0.9 can be used for devices with fixed addresses.

The gateway will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address is the gateway's LAN IP address
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the gateway's LAN IP address
- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu.



**Note:** The gateway implements a DNS Relay function. When it receives a DNS request on the LAN, it passes it to the DNS server specified on the WAN. It then relays the response back to the original requesting PC.

## Viewing and Emailing Logged Information

The gateway will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering, the Logs page shows you when someone on your network tried to access a blocked site. You can enable e-mail notification to receive these logs in an e-mail message. An example is shown below.

The screenshot shows a web-based configuration interface for a 'Content Filtering' section. On the left, a sidebar lists 'Logs', 'Block Sites', and 'Services'. The main area is titled 'Logs' and contains fields for 'Contact Email Address' and 'SMTP Server Name', both with empty input boxes. Below these are 'E-mail Alerts' settings, including an unchecked checkbox labeled 'Enable' and a 'Apply' button. At the bottom are buttons for 'E-mail Log' and 'Clear Log'.

Description	Count	Last Occurrence	Target	Source
-------------	-------	-----------------	--------	--------

E-mail Log | Clear Log

**Figure 5-3: Logs menu**

Log entries are described in [Table 5-4](#)

**Table 5-4: Security Log entry descriptions**

Field	Description
Description	The type of event and what action was taken if any.
Count	This is a reference number for each event.
Last Occurrence	The date and time the log entry was recorded.
Target	The name or IP address of the destination device or website.
Source	The IP address of the initiating device for this log entry.

## **Enabling Logs Event E-mail Notification**

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the E-Mail section of the Logs menu:

- In the Contact Email Address, type the e-mail address to which the logs will be sent. Use a full e-mail address (for example, ChrisXY@myISP.com).
- In the SMTP Server Name box, type the outgoing SMTP mail server of your ISP (for example, mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, no alerts or logs will be sent.
- Check the E-mail Alerts Enable box.
- Click E-mail Log to send the log immediately.
- Click Apply

## **Erasing Configuration**

---

The configuration settings of the CG814M Gateway are stored in a configuration file in the gateway. This file can be reverted to factory default settings. The procedures below explain how to do these tasks.

It is sometimes desirable to restore the gateway to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Main Menu, under Maintenance select Set Password. Select Yes for Restore Factory Defaults and click Apply.
2. The gateway will then reboot automatically.

After an erase, the gateway's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

**Note:** To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the gateway.

1. Using a paper clip, depress and hold the Default Reset Button. All the numbered Ethernet LEDs will illuminate green.
2. Continue to depress the button for at least 5 seconds.
3. The gateway will reboot and clear its configuration information.

## Running Diagnostic Utilities

The CG814M Gateway has a diagnostics feature. You can use the diagnostics menu to test connectivity to PC using the Ping command:

From the Main Menu of the browser interface, under the Maintenance heading, select the Diagnostics menu, shown in [Figure 5-5](#).

The screenshot shows the 'Diagnostics' page under the 'Maintenance' menu. The left sidebar lists 'Gateway Status', 'Connection', 'Set Password', and 'Diagnostics'. The main area is titled 'Diagnostics' and contains 'Ping Test Parameters' with fields for 'Ping Target' (192.168.0.10), 'Ping Size' (64 bytes), 'No. of Pings' (3), and 'Ping Interval' (1000 ms). Below are three buttons: 'Start Test', 'Abort Test', and 'Clear Results'. A large text box displays the results of a ping test to 192.168.0.10, showing three replies received with a minimum time of 10 ms, maximum time of 10 ms, and average time of 0 ms. At the bottom, a red message says 'To get an update of the results you must [REFRESH](#) the page.'

**Figure 5-5: Diagnostics menu**

To perform a Ping test

1. In the Ping Target section, enter the IP address of the PC you would like to ping.
2. If you would like to specify additional details, you can set the Ping Size, No. of Ping and Ping Interval.
3. Click Start Test.
4. Click REFRESH to see the results of the Ping test.



## **Chapter 6**

# **Troubleshooting**

This chapter gives information about troubleshooting your CG814M Wireless Cable Modem Gateway. For the common problems listed, go to the section indicated.

- Is the gateway on?
- Have I connected the gateway correctly?

Go to “[Basic Functions](#)“ on page 6-1.

- I can’t access the gateway’s configuration with my browser.

Go to “[Troubleshooting the Web Configuration Interface](#)“ on page 6-3.

- I’ve configured the gateway but I can’t access the Internet.

Go to “[Troubleshooting the ISP Connection](#)“ on page 6-4.

- I can’t remember the gateway’s configuration password.
- I want to clear the configuration and start over again.

Go to “[Erasing Configuration](#)“ on page 5-8.

## **Basic Functions**

---

After you turn on power to the gateway, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. Verify that the numbered ethernet LEDs come on momentarily.
3. After approximately 30 seconds, verify that:
  - c. The Local port Link LEDs are lit for any local ports that are connected.
  - d. The Test LED is not lit.

- e. The Internet Link port LED is lit.

If any of these conditions does not occur, refer to the appropriate following section.

## **Power LED Not On**

If the Power and other LEDs are off when your gateway is turned on:

- Make sure that the power cord is properly connected to your gateway and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

## **Test LED Stays On**

If the Test LED stays on continuously, there is a fault within the gateway.

If you experience problems with the Test LED:

- Cycle the power to see if the gateway recovers and the LED goes off
- If all LEDs including the Test LED are still on one minute after power up, clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in "["Erasing Configuration" on page 5-8](#).

If the error persists, you might have a hardware problem and should contact technical support.

## **Local Link LEDs Not On**

If the Local Port Link LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the gateway and at the hub or PC.
- Make sure that power is turned on to the connected hub or PC.
- Be sure you are using the correct cable:
  - When connecting the gateway's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

## Cable Link LED Not On

If the Cable Link LED does not light when connected to your cable television cable, check the following:

- Make sure that the coaxial cable connections are secure at the gateway and at the wall jack.
- Make sure that your cable internet service has been provisioned by your cable service provider. Your provider should verify that the signal quality is good enough for cable modem service.
- Remove any excessive splitters you may have on your cable line. It may be necessary to run a “home run” back to the point where the cable enters your home.

## Troubleshooting the Web Configuration Interface

---

If you are unable to access the gateway’s Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the gateway as described in the previous section.
- Make sure your PC’s IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your PC’s address should be in the range of 192.168.0.10 to 192.168.0.254. Refer to “[Verifying TCP/IP Properties](#)“ on page C-5 or “[Configuring the Macintosh for TCP/IP Networking](#)“ on page C-6 to find your PC’s IP address. Follow the instructions in [Appendix C](#) to configure your PC.

**Note:** If your PC’s IP address is shown as 169.254.x.x:

Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the gateway and reboot your PC.

- If your gateway’s IP address has been changed and you don’t know the current IP address, clear the gateway’s configuration to factory defaults. This will set the gateway’s IP address to 192.168.0.1. This procedure is explained in “[Erasing Configuration](#)“ on page 5-8.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.

- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the gateway does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

## **Troubleshooting the ISP Connection**

---

If your gateway is unable to access the Internet and your Cable Link LED is on, you may need to register the Cable MAC Address and/or Device MAC Address of your gateway with your cable service provider. This is described in “[Configuration](#)” on page 2-11.

Additionally, your PC may not have the gateway configured as its TCP/IP gateway. If your PC obtains its information from the gateway by DHCP, reboot the PC and verify the gateway address as described in “[Verifying TCP/IP Properties](#)” on page C-6.

## **Troubleshooting a TCP/IP Network Using a Ping Utility**

---

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made easier by using the ping utility in your PC or workstation.

### **Testing the LAN Path to Your Gateway**

You can ping the gateway from your PC to verify that the LAN path to your gateway is set up correctly.

To ping the gateway from a PC running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the gateway, as in this example:

```
ping 192.168.0.1
```

3. Click on OK.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in “[Local Link LEDs Not On](#)” on page 6-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your gateway and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <IP address> is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your gateway listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway as described in “[Verifying TCP/IP Properties](#)“ on page C-6.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your Cable Link LED is on.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Device MAC Address of your gateway because it does not match the MAC Address of the PC you previously used to connect to a cable modem. In this case you will need to clone your PCs MAC Address. Refer to “[Configuration](#)“ on [page 2-11](#).

## **Appendix A**

# **Technical Specifications**

This appendix provides technical specifications for the CG814M Wireless Cable Modem Gateway.

### **Network Protocol and Standards Compatibility**

Data and Routing Protocols:	TCP/IP DHCP server and client DNS relay NAT (many-to-one) TFTP client VPN pass through (IPSec, L2TP)
-----------------------------	---

### **Power Adapter**

North America (input):	120V, 60 Hz, input
All regions (output):	12 V DC @ 1.25A output, 20W maximum

### **Physical Specifications**

Dimensions:	255 by 169 by 34 mm 10.0 by 6.7 by 1.3 in.
Weight:	0.54 kg 1.2 lb.

### **Environmental Specifications**

Operating temperature:	32°-140° F (0° to 40° C)
Operating humidity:	90% maximum relative humidity, noncondensing

### **Electromagnetic Emissions**

Meets requirements of:	FCC Part 15 Class B
------------------------	---------------------

### **Interface Specifications**

---

Local:	10BASE-T or 100BASE-Tx, RJ-45 USB 1.1 Function 802.11b Wireless Access Point
Internet:	DOCSIS 1.0, upgradeable to DOCSIS 1.1

---

## **Appendix B**

# **Networks, Routing, and Firewall Basics**

This chapter provides an overview of IP networks, routing, and firewalls.

## **Related Publications**

---

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at [www.ietf.org](http://www.ietf.org) and are mirrored and indexed at many other sites worldwide.

## **Basic Router Concepts**

---

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

## **What is a Router?**

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The CG814M Wireless Cable Modem Gateway is a small office router that routes the IP protocol over a single-user broadband connection.

## **Routing Information Protocol**

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The CG814M Gateway supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

## **IP Addresses and the Internet**

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at [www.iana.org](http://www.iana.org).

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

11000011 00100010 00001100 00000111

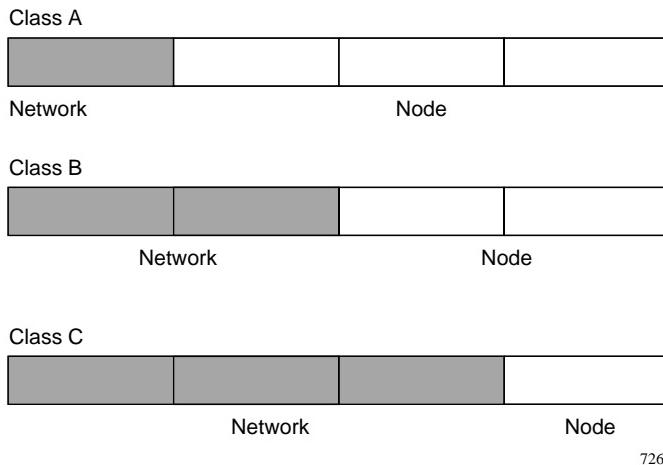
is normally written as:

195.34.12.7

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.



**Figure 6-1: Three Main Address Classes**

The five address classes are:

- **Class A**

Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

`1.x.x.x to 126.x.x.x`.

- **Class B**

Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

`128.1.x.x to 191.254.x.x`.

- Class C

Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

192.0.1.x to 223.255.254.x.

- Class D

Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

224.0.0.0 to 239.255.255.255.

- Class E

Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

## **Netmask**

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

11000000 10101000 10101010 11101101 (192.168.170.237)

combined with:

11111111 11111111 11111111 00000000 (255.255.255.0)

Equals:

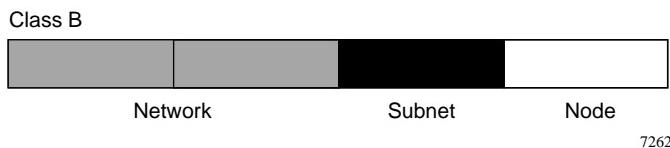
11000000 10101000 10101010 00000000 (192.168.170.0)

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

## **Subnet Addressing**

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.



**Figure 6-2: Example of Subnetting a Class B Address**

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

**Table 6-1. Netmask Notation Translation Table for One Octet**

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the mask length formats.

**Table 6-2. Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

**Table 6-2. Netmask Formats**

255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

## Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 – 10.255.255.255  
172.16.0.0 – 172.31.255.255  
192.168.0.0 – 192.168.255.255

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the CG814M Gateway is preconfigured to automatically assign private addresses.

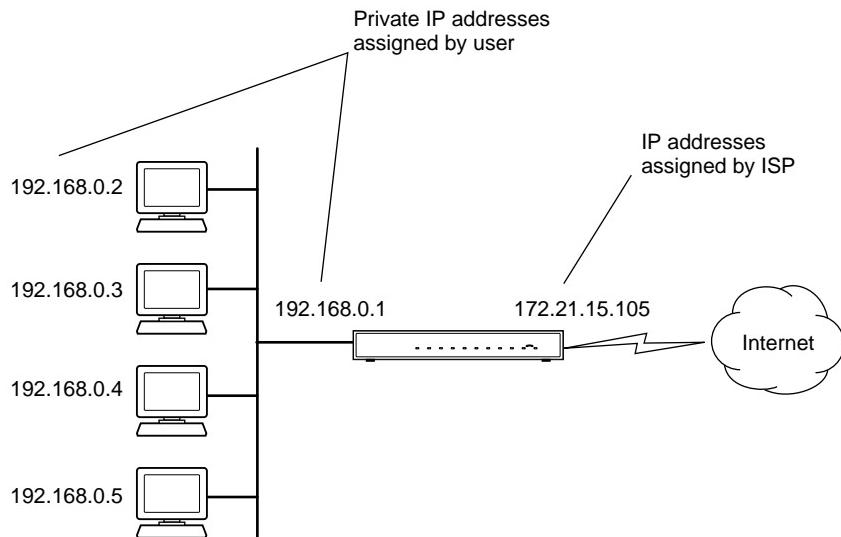
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at [www.ietf.org](http://www.ietf.org).

## Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The CG814M Gateway employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.



7786EA

**Figure 6-3: Single IP Address Operation Using NAT**

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

## **MAC Addresses and Address Resolution Protocol**

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

## **Related Documents**

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

## **Domain Name Server**

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

## **IP Configuration by DHCP**

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The CG814M Gateway has the capacity to act as a DHCP server.

The CG814M Gateway also functions as a DHCP client when connecting to the ISP. The gateway can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

## **Internet Security and Firewalls**

---

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

## **What is a Firewall?**

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

## **Stateful Packet Inspection**

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection "states." Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

## **Denial of Service Attack**

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

## Wireless Networking

---

The CG814M Gateway conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11b devices.

## Wireless Network Configuration

The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

### Ad-hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft Networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as Peer-to-Peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

### Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

## **Extended Service Set Identification (ESSID)**

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad-hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the Extended Service Set Identification (ESSID) is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

## **Authentication and WEP Encryption**

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is utilized when the wireless nodes or access points are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configured). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

## Wireless Channel Selection

IEEE 802.11b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4Ghz and 2.5Ghz. Neighboring channels are 5Mhz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5Mhz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in [Table B-1](#):

**Table B-1. 802.11b Radio Frequency Channels**

Channel	Center Frequency	Frequency Spread
1	2412Mhz	2399.5Mhz - 2424.5Mhz
2	2417Mhz	2404.5Mhz - 2429.5Mhz
3	2422Mhz	2409.5Mhz - 2434.5Mhz
4	2427Mhz	2414.5Mhz - 2439.5Mhz
5	2432Mhz	2419.5Mhz - 2444.5Mhz
6	2437Mhz	2424.5Mhz - 2449.5Mhz
7	2442Mhz	2429.5Mhz - 2454.5Mhz
8	2447Mhz	2434.5Mhz - 2459.5Mhz
9	2452Mhz	2439.5Mhz - 2464.5Mhz
10	2457Mhz	2444.5Mhz - 2469.5Mhz
11	2462Mhz	2449.5Mhz - 2474.5Mhz
12	2467Mhz	2454.5Mhz - 2479.5Mhz
13	2472Mhz	2459.5Mhz - 2484.5Mhz

**Note:** The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

## Ethernet Cabling

---

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring as described in [Table 6-1](#).

**Table 6-1. UTP Ethernet cable wiring, straight-through**

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

## Uplink Switches and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs

are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

## **Cable Quality**

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

## **Appendix C**

### **Preparing Your Network**

This appendix describes how to prepare your network to connect to the Internet through the CG814M Wireless Cable Modem Gateway and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).



**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your gateway. Write down this information before reconfiguring your computers. Refer to “[Obtaining ISP Configuration Information for Windows Computers](#)” on page C-10 or “[Obtaining ISP Configuration Information for Macintosh Computers](#)” on page C-11 for further information.

### **Preparing Your Computers for TCP/IP Networking**

---

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the gateway must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to “[Appendix B, “Networks, Routing, and Firewall Basics.”](#)

The CG814M Gateway is shipped preconfigured as a DHCP server. The gateway assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the gateway)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

## **Configuring Windows 95, 98, and ME for TCP/IP Networking**

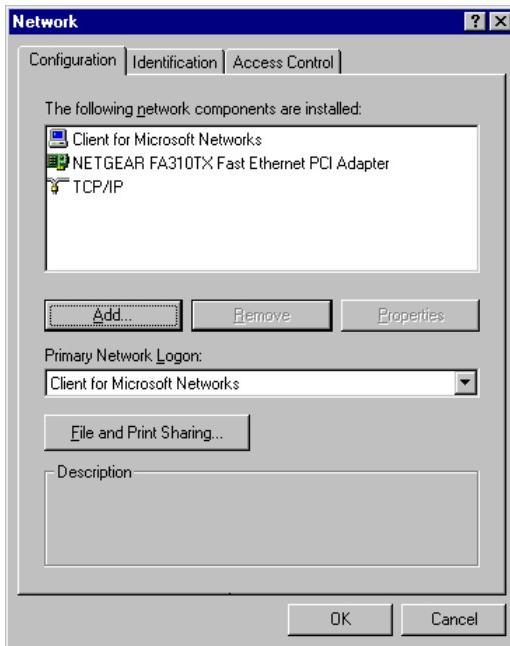
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **Install or Verify Windows Networking Components**

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.



**Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

- a. Click the Add button.
- b. Select Adapter, and then click Add.
- c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

- a. Click the Add button.
- b. Select Protocol, and then click Add.
- c. Select Microsoft.
- d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

- a. Click the Add button.
  - b. Select Client, and then click Add.
  - c. Select Microsoft.
  - d. Select Client for Microsoft Networks, and then click OK.
3. Restart your PC for the changes to take effect.

### **Enabling DHCP to Automatically Configure TCP/IP Settings**

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the CG814M Gateway. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the gateway, then restart the gateway and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

### **Selecting Windows’ Internet Access Method**

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.

5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

## **Verifying TCP/IP Properties**

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

## **Configuring Windows NT, 2000 or XP for IP Networking**

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **Install or Verify Windows Networking Components**

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.

5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Make sure your PC is connected to the gateway, then reboot your PC.

## **Verifying TCP/IP Properties**

To check your PC’s TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.  
The Run window opens.
2. Type `cmd` and then click OK.  
A command window opens
3. Type `ipconfig /all`

Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP address is between 192.168.0.2 and 192.168.0.254
  - The subnet mask is 255.255.255.0
  - The default gateway is 192.168.0.1
4. Type `exit`

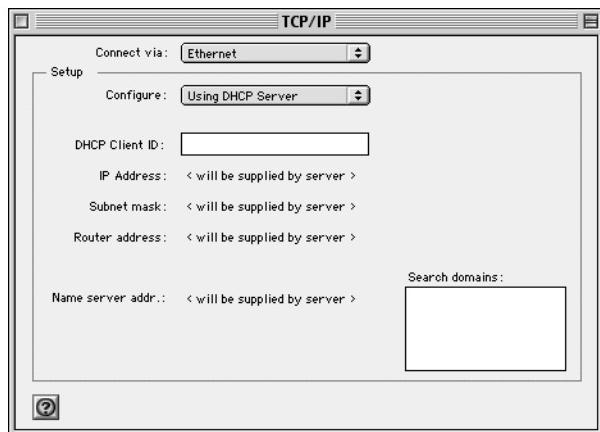
## **Configuring the Macintosh for TCP/IP Networking**

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

### **MacOS 8.6 or 9.x**

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens:



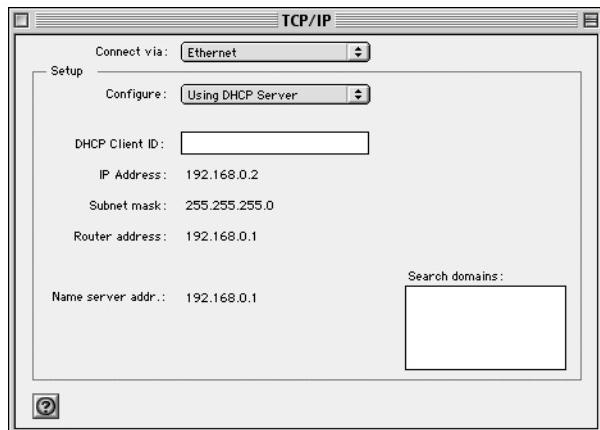
2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.  
You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

## **MacOS X**

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

## **Verifying TCP/IP Properties for Macintosh Computers**

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

## **Verifying the Readiness of Your Internet Account**

---

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your gateway takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the gateway's Internet port is connected to the broadband modem, the gateway appears to be a single PC to the ISP. The gateway then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the gateway to accomplish this is called Network Address Translation (NAT) or IP masquerading.

## **What Is Your Configuration Information?**

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

For example, your account's full server names may look like this:

mail.xxx.yyy.com

In this example, the domain suffix is xxx.yyy.com.

If any of these items are dynamically supplied by the ISP, your gateway automatically acquires them.

If an ISP technician configured your PC during the installation of the cable modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the gateway. These procedures are described next.

## **Obtaining ISP Configuration Information for Windows Computers**

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the CG814M Gateway. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the gateway for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components.

3. Select TCP/IP, and then click Properties.

The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".

5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

## **Obtaining ISP Configuration Information for Macintosh Computers**

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the CG814M Gateway. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the gateway for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

## **Restarting the Network**

---

Once you've set up your computers to work with the gateway, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your CG814M Gateway, you are ready to access and configure the gateway.

## Glossary

<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
<b>100BASE-Tx</b>	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
<b>802.11b</b>	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
<b>Denial of Service attack</b>	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
<b>DHCP</b>	<i>See</i> Dynamic Host Configuration Protocol.
<b>DNS</b>	<i>See</i> Domain Name Server.
<b>domain name</b>	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
<b>DOCSIS</b>	Data Over Cable Service Interface Specification. Defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks
<b>Domain Name Server</b>	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
<b>Dynamic Host Configuration Protocol</b>	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

<b>Gateway</b>	A local device, usually a router, that connects hosts on a local network to other networks.
<b>IETF</b>	Internet Engineering Task Force. An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at <a href="http://www.ietf.org">www.ietf.org</a> .
<b>IP</b>	Internet Protocol. The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
<b>IP Address</b>	A four-position number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
<b>IPSec</b>	Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.
<b>ISP</b>	Internet service provider.
<b>LAN</b>	<i>See</i> local area network.
<b>local area network</b>	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
<b>MAC address</b>	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
<b>Mbps</b>	Megabits per second.
<b>MSB</b>	<i>See</i> Most Significant Bit or Most Significant Byte.
<b>MTU</b>	<i>See</i> Maximum Transmit Unit.
<b>Maximum Transmit Unit</b>	The size in bytes of the largest packet that can be sent or received.
<b>Most Significant Bit or Most Significant Byte</b>	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

<b>NAT</b>	<i>See</i> Network Address Translation.
<b>netmask</b>	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
<b>Network Address Translation</b>	A technique by which several hosts share a single IP address for access to the Internet.
<b>packet</b>	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
<b>PPP</b>	<i>See</i> Point-to-Point Protocol.
<b>PPTP</b>	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
<b>Point-to-Point Protocol</b>	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
<b>RFC</b>	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at <a href="http://www.ietf.org">www.ietf.org</a> .
<b>RIP</b>	<i>See</i> Routing Information Protocol.
<b>router</b>	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
<b>Routing Information Protocol</b>	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
<b>subnet mask</b>	<i>See</i> netmask.
<b>URL</b>	Universal Resource Locator, the global address of documents and other resources on the World Wide Web.
<b>UTP</b>	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

<b>VPN</b>	Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.
<b>WAN</b>	<i>See</i> wide area network.
<b>WEP</b>	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
<b>wide area network</b>	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
<b>Windows Internet Naming Service</b>	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.
<b>WINS</b>	<i>See</i> Windows Internet Naming Service.